HP LeftHand SAN Solutions

Support Document

Best Practices

Best Practice for Active Monitoring of LeftHand SANs

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

© Copyright 2009 Hewlett-Packard Development Company, L.P.

Best Practices for Active Monitoring of the LeftHand SAN

Overview

Active monitoring is a critically important feature of the SAN/iQ software installed on Network Storage Modules (NSMs). Active monitoring enables you to track the health of NSMs. Email notifications and/or SNMP traps are generated by NSMs to alert you to critical system events. Events are also displayed in the Alerts tab of the Reporting category in the Centralized Management Console (Console). Examples of alert events include: volume offline, power supply failure, disk failure, etc.

The LeftHand SAN User Manual describes in detail how to configure active monitoring. These best practices describe the overall approach to implementing active monitoring and recommendations regarding the implementation and management of active monitoring.

Use a Phased Approach

A complete monitoring solution uses both the NSMs to notify administrators of system events, as well as an additional external monitoring system to determine the availability of the NSMs.

This external monitoring system is necessary because a power or network failure can make all NSMs unavailable, and prevent them from sending a message indicating that there is a problem. In this case, an external monitoring system will determine that the NSMs are unavailable and send an appropriate warning.

When planning a monitoring configuration, it is important to take a "crawl, walk, run" approach by starting simple and expanding coverage in phased steps. A phased implementation avoids the common problem of planning a complete SNMP monitoring system, purchasing monitoring hardware and software, and then never getting the system configured because it ends up being such a large project.

Given this, we recommend the following phased approach:

1. Create a mail alias for email alerts.
2. Configure basic external monitoring.
3. Configure basic email alerts.
4. Test the availability of critical component services.
5. Configure NSMs for SNMP Traps

Create a Mail Alias for Email Alerts

In general, it is best to create a new mail alias specifically for email alerts (e.g., nsmalerts@ example.com). By using a unique address instead of creating a list of individual addresses, you can centrally manage the recipients of the email alerts, and you will not need to change the monitoring configuration on each NSM if you have a staffing change, a network change, etc.

NOTE: If your mail server uses the NSMs for storage, consider using another system capable of delivering mail for handling the NSM email alerts. If the NSMs experience a problem and attempt to send mail to a mail server that is using the IP SAN for storage, the delivery of the alert message may be delayed until the problem on the NSM is repaired.

Configure Basic External Monitoring

Basic external monitoring is usually trivial to configure and provides a regular basic check of your IP SAN. Basic external monitoring consists of using network pings at periodic intervals (e.g., once per minute), and providing notification on failure. It is often best to define "failure" as several consecutive failed pings in order to avoid false alarms due to transient network problems. Third party software – for example, Ipswitch WhatsUp Gold (*) – can do this basic monitoring.

Your monitoring station requires access to the NSMs. If your NSMs are on a non-routable dedicated network, you need to add another network interface to your monitoring station for the IP SAN subnet.

Configure Basic Email Alerts

1. Configure Email Alerts

Configure an SMTP server address under the Email tab of the Reporting category in the Console. You will also need to configure the "From" address to get your mail server/relays to accept the alert messages.

2 Test Email Alert Configuration

— On platforms with dual power supplies (e.g., NSM200)

To test this, you'll need to generate an alert.

– Configure the Power Supply Status alert with your personal email address.

– Press the button on the back of the NSM to switch power supplies, or simply remove one of the power supplies.

– You should see an alert in the Alerts tab of the Reporting category in the Console, and receive email notification within a minute or so.

– Note: Be sure to wait long enough for the system to generate the email notification. If you press the button twice within 60 seconds, an alert may not be generated because the switch was so rapid that it was not recognized as a state change by the monitoring system.

– Return the power supplies to their original state when you have finished verifying the email configuration.

— On platforms with single power supply (e.g., NSM150)

To generate an alert on platforms with a single power supply

– Verify that the network settings on the NSM are configured for Active-Backup bond.

– Then unplug one of the network cables.

You should see an alert in the Alerts tab of the Reporting category in the Console, and receive email notification within a minute or so.

– Plug in the network cable when you have finished verifying the email configuration.

3 Copy the email alerts configuration to other NSMs.

— Use Copy Configuration to copy monitoring configurations from one NSM to other NSMs.

- In the Network View, right-click on the NSM that is configured for email alerts.
- Select Copy Configuration from the menu to open the Copy Configuration dialog.
- Select the Configuration Settings to copy in the top section and the NSMs to receive the configuration settings in the bottom section.
- Click copy. The selected configurations are copied to the selected NSMs.

4. 4. Next, use the instructions in Step 2 to test the alert configurations on each of the other NSMs.
5. Configure email alerts for all the monitoring variables and copy those to other NSMs.

Note: An enhancement request is under consideration for future releases of the SAN/iQ software (after version 6.3) to provide a way to differentiate between critical, warning, and informational alerts.

Test the Availability of Critical Component Services

There are three critical component services on each NSM: Configuration service, Storage service, and (optionally) the Manager service. The availability of these services can be determined by connecting to their associated TCP ports. Third party software – for example, Ipswitch WhatsUp Gold (*) – can be configured to monitor these ports.

The TCP port numbers for these services are:

- Configuration Service: 13838
- Storage Service: 13847
- Manager Service: 13846

If any of these connections fail, that failure indicates that the component failing to respond is not available and may have a problem. Again, a "failure" should be defined as several failed connection attempts in a row because normal operations can result in these services being unavailable for a few minutes or so.

Configure NSMs for SNMP Traps

Finally, NSMs can be configured to generate SNMP traps. The LeftHand SAN User Manual describes how to configure this feature. This section describes the most useful application of traps with respect to NSMs.

A monitoring solution like HP OpenView that can accept SNMP traps can be used to log, aggregate, correlate, report, and provide notification of these events. It may also be possible to take custom actions or use different notification methods based on a specific type of event. Your SNMP monitoring system may support using a series of methods to deliver notification messages.

Consider configuring your monitoring system to contact you in the event that your email server or Internet connection is unavailable. Traditionally, this is a multiphase approach that first uses internal email, then email directly to pagers/phones over the Internet, and finally analog phone calls to pagers/phones.

(*) NOTE: Third-party software applications that are mentioned in this article (e.g., Ipswitch WhatsUp Gold) are listed as examples only. LeftHand Networks, Inc. does not endorse or provide support for these products.